-2-

MIKOS-101                        09/778,967                      07650001aa
Amendment dated 11/03/2005              Reply to office action mailed 05/04/2005


The following is a complete listing of all claims in the application, with an

indication of the status of each:


<u>Listing of claims:</u>


1       1. (currently amended)  System for authenticating digital information,

2       comprising:

3              a) an image acquisition device for producing an original array of

4       two-dimensional digital information;

5              b) means for obtaining current date and time information from satellite

6       or radio broadcasts;

7              c) means for obtaining current location information from satellite or

8       radio broadcasts;

9              d) means for identifying a Sensor ID for the image acquisition device;

10             e) an encoder for converting date/time, location, and Sensor ID into

11      two-dimensional format called the Encoded Data Array;

12             f) an embedder for combining the Encoded Data Array and the

13      Original Array into a new Composite Array

14             h) a Transmission device to transfer the Composite Array to a

15      recipient;

16             n) means for comparing said transferred Composite Array to said

17      Encoded Data Array, said comparing means thereby being able to determine

18      whether said Encoded Data Array is embedded in said Composite Array, <u>said</u>

19      <u>comparing means being further limited by being able to make said</u>

20      <u>determination without extracting or otherwise decoding information in said</u>

21      <u>Encoded Data Array;</u>

22             j) a decoder with fault indicator when date/time, location, and source

23      cannot be decoded;

-3-

MIKOS-101                          09/778,967                        07650001aa
Amendment dated 11/03/2005          Reply to office action mailed 05/04/2005

24          k) an Encoding Extractor for removing the Encoded Data Array from

25     the Composite Array;

26          l) means for restoring the Original Array at pixel locations used for the

27     Encoding; and

28          m) means for determining changes between the Restored Original

29     Array and the Original Array.


1      2. (previously presented)  System as in Claim 1 in which the Original Array

2      size is increased by a factor and subpixels are used in steps f, h, n, j, k, l, and

3      m.


1      3. (previously presented)  System as in claim 20 in which the encryption of

2      step g and decryption of step i is repeated more than one time.


1      4. (previously presented)  System as in Claims 1 or 2 in which the encryption

2      process involves scrambling the pixels or subpixels.


1      5. (previously presented)  System as in Claims 1 or 2 in which steps b and c

2      utilize the GPS (Global Positioning Satellite) system.


1      6. (previously presented)  System as in Claims 1 or 2 in which the Decoder

2      utilizes flash correlation to select pixel locations of the Encoded Data Array

3      and test for authenticity.


1      7. (previously presented)  System as in Claims 1 or 2 in which the Sensor ID

2      in step d includes a biometric identifier of the User of the image acquisition

3      device.

-4-

MIKOS-101                          09/778,967                    0765000laa
Amendment dated 11/03/2005        Reply to office action mailed 05/04/2005

1       8. (previously presented) System as in Claims 1 or 2 in which the Sensor ID
2       in step d includes the serial number and odometer setting of the image
3       acquisition device of step a.

1       9. (previously presented) System as in Claims 1 or 2 in which the change
2       detector of step m evaluates subsections of the Restored Original Array and
3       the Original Array to localize areas of difference.

1       10. (previously presented) System as in Claim 6 in which flash correlation is
2       used to verify that the encoded data is the same as data which is expected to
3       be encoded into a particular Original Array.

1       11. (previously presented) System as in Claim 6 in which flash correlation is
2       used to identify the encoded data by exhaustive comparison against each
3       possible value for each of date/time, location, and source.

1       12. (previously presented) System as in Claims 1 or 2 in which date/time,
2       location, and source are annotated onto the Encrypted Composite Array.

1       13. (previously presented) System as in Claims 1 or 2 in which the encoded
2       data provides the key to the encryption and decryption algorithms.

1       14. (previously presented) System of Claims 1 or 2 in which the operation of
2       the image acquisition device is triggered by the change of status of another
3       device.

1       15. (original) System of Claim 14 in which the triggering device is a face
2       recognition system.

-5-

MIKOS-101                                09/778,967                                07650001aa
Amendment dated 11/03/2005         Reply to office action mailed 05/04/2005

1      16. (original) System of Claim 14 in which the triggering device is a speed

2      sensor.


1      17. (original) System of Claim 14 in which the triggering device is an alarm

2      condition sensor.


1      18. (previously presented) System of Claims 1 or 2 in which the Encoding is

2      performed by overlaying a pattern of pixels of a particular color or grey scale

3      value.


1      19. (previously presented) System of Claims 1 or 2 in which the Encoding is

2      performed by steganography.


1      20. (previously presented) System of Claims 1 or 2, further comprising:

2              g) an encrypter for encrypting the Composite Array;

3              i) a decrypter to restore the Composite Array.


1      21. (currently amended) A method for authenticating digital images,

2      comprising the steps of:

3              capturing a digital image;

4              recording authentication information at the time and place of said

5      capturing, said authentication information being unique to said digital image

6      and including at least one piece of information from a source independent of

7      said capturing;

8              encoding said authentication information into a data array mapable to

9      said digital image;

MIKOS-101                           09/778,967                        07650001aa
Amendment dated 11/03/2005          Reply to office action mailed 05/04/2005

10          mapping said data array to said digital image, thereby creating a

11     composite array;

12          optionally encrypting said composite array;

13          optionally annotating said composite array;

14          comparing said data array, optionally encrypted and annotated, to a

15     target composite array, wherein said comparing determines whether said

16     authentication information is embedded in said target composite array, said

17     comparing being further limited by being able to make said determination

18     without extracting or otherwise decoding information in said data array,

19     thereby proving that said target composite array is an authentic copy of said

20     composite array.


1      22. (original) The method of claim 21, wherein said at least one piece of

2      information from a source independent of said capturing is GMT time

3      information.


1      23. (original) The method of claim 21, wherein said at least one piece of

2      information from a source independent of said capturing is GPS location

3      information.


1      24. (original) The method of claim 21, wherein said at least one piece of

2      information from a source independent of said capturing is GMT time

3      information and GPS location information.


1      25. (previously presented) The method of claim 21, wherein said comparing

2      step is flash correlation of said data array with said target composite array.

-7-

MIKOS-101                          09/778,967                          07650001aa
Amendment dated 11/03/2005                    Reply to office action mailed 05/04/2005

1       26. (previously presented)  The method of claim 25, wherein said digital

2       image is a sequence of digital images, there being a unique set of

3       authenticating information for each digital image in said sequence and a

4       corresponding unique data array, there being a unique composite array

5       corresponding to each digital image in said sequence, wherein said composite

6       array is a sequence of composite arrays and said target composite array is a

7       sequence of target composite arrays, and wherein said flash correlation

8       determines whether said sequence of target composite arrays is an authentic

9       copy of said sequence of composite arrays.

1       27. (previously presented)  The method of claim 26, wherein said sequence of

2       digital images is a video image and said flash correlation is done in real time.

1       28. (currently amended)  A system for authenticating digital images,

2       comprising:

3           means for capturing a digital image;

4           means for recording authentication information at the time and place

5       of said capturing, said authentication information being unique to said digital

6       image and including at least one piece of information from a source

7       independent of said capturing;

8           means for encoding said authentication information into a data array

9       mapable to said digital image;

10           means for mapping said data array to said digital image, thereby

11       creating a composite array;

12           means for optionally encrypting said composite array;

13           means for optionally annotating said composite array;

14           means for comparing said data array, optionally encrypted and

15       annotated, to a target composite array, wherein said comparing determines

-8-

MIKOS-101                    09/778,967                      07650001aa
Amendment dated 11/03/2005         Reply to office action mailed 05/04/2005

16    whether said authentication information is embedded in said target composite

17    array, said comparing means being further limited by being able to make said

18    determination without extracting or otherwise decoding information in said

19    data array, thereby proving that said target composite array is an authentic

20    copy of said composite array.


1     29. (original)  The system of claim 28, wherein said at least one piece of

2     information from a source independent of said capturing is GMT time

3     information.


1     30. (original)  The system of claim 28, wherein said at least one piece of

2     information from a source independent of said capturing is GPS location

3     information.


1     31. (original)  The system of claim 28, wherein said at least one piece of

2     information from a source independent of said capturing is GMT time

3     information and GPS location information.


1     32. (previously presented)  The system of claim 28, wherein said comparing

2     step is flash correlation of said data array with said target composite array.


1     33. (previously presented)  The system of claim 32, wherein said digital

2     image is a sequence of digital images, there being a unique set of

3     authenticating information for each digital image in said sequence and a

4     corresponding unique data array, there being a unique composite array

5     corresponding to each digital image in said sequence, wherein said composite

6     array is a sequence of composite arrays and said target composite array is a

7     sequence of target composite arrays, and wherein said flash correlation

-9-

MIKOS-101                          09/778,967                          07650001aa
Amendment dated 11/03/2005                    Reply to office action mailed 05/04/2005


8        determines whether said sequence of target composite arrays is an authentic

9        copy of said sequence of composite arrays.


1        34. (previously presented)  The system of claim 33, wherein said sequence of

2        digital images is a video image and said flash correlation is done in real time.